PX 256

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
NEW YORK REGIONAL OFFICE
200 Vesey Street, Suite 400
New York, NY 10281-1022

DIVISION OF ENFORCEMENT

Daphna A. Waxman
(212) 336-1012
waxmand@sec.gov

April 13, 2018

Via Email (meredith.cross@wilmerhale.com)

Ripple Labs, Inc.
c/o Meredith B. Cross, Esq.
WilmerHale
1875 Pennsylvania Avenue NW
Washington, DC 20006

Re: Ripple (MNY-9875)

Dear Ms. Cross:

We believe Ripple Labs, Inc. ("Ripple"), and any affiliated entities, may possess documents and data that are relevant to the above referenced non-public, investigation being conducted by the staff of the Division of Enforcement. Accordingly, we hereby provide notice that Ripple shall reasonably preserve and retain such evidence until further notice. Failure to do so could give rise to civil and criminal liability.

The Commission considers potentially relevant documents that relate or refer to:

(1) the structure, management, and operation of Ripple;

(2) the creation, issuance, offer or sale of XRP Tokens;

(3) the promotion or marketing of XRP Tokens by Ripple or any other entity on behalf of Ripple;

(4) the trading of XRP Tokens on any digital asset platform;

(5) any analysis by Ripple to determine whether the XRP Token is a "security" within the meaning of the U.S. federal securities laws; and/or

(ii) the application of the U.S. securities laws to the offer, purchase, or sale of XRP Tokens; and

(6) any statement made by Ripple or on behalf of Ripple regarding XRP Tokens.

Such documents include both "hard copy" versions and electronically-stored information in Ripple's possession, custody or control, including text files, data compilations, word processing documents, spreadsheets, e-mail, voicemail, data bases, calendars and scheduling information, logs, file fragments and backup files, letters, instant messages, memoranda, notes, drawings, designs, correspondence or communication of any kind. Evidence that is stored electronically may be maintained on shared network files, computer hard drives, servers, DVDs, CD-ROMs, flash drives, thumb drives, laptops, digital recorders, netbooks, PDAs, smartphones, or other handheld devices.

In this letter, I refer to such documents and data as "Evidence." Your client has a duty to reasonably preserve and retain such Evidence.

This duty includes an obligation to provide notice to all employees or custodians who may be in possession of Evidence. This duty also extends to the preservation and retention of Evidence in the possession or custody of third-parties, such as an internet service provider or a cloud computing provider, if such Evidence is within Ripple's control.

Your client may need to act affirmatively to prevent the destruction of Evidence. This duty may necessitate quarantining certain Evidence to avoid its destruction or alteration. Your client should consider whether they need to discontinue the routine destruction of Evidence, including discontinuing the recycling of backup tapes or other storage media, and the deletion of emails, "trash," "recycling," "drafts," "sent," or "archived" folders. Your client should avoid running or installing any drive cleaning, wiping, encrypting, or defragmenting software on hard disks of computers that may contain Evidence.

Your client should consider preserving any forensically recoverable data by having mirror image copies made of the Evidence. Having said that, any attempt to replicate electronic data without adhering to best practices for data replication could compromise the integrity or contents of such data. Simply making "hard copies" of such Evidence or transforming it to other formats (such as TIFF, or PDF documents) does not constitute preservation of such Evidence. We are prepared to discuss with you proper protocols for replication before you attempt to copy Evidence. The Commission may be able to retain and supervise computer forensic resources to properly and non-invasively create back-up images of Evidence.

In addition to preserving the Evidence described above, we further request that Ripple take no action to delete or otherwise compromise any content existing on social networking websites such as "Facebook" or "LinkedIn." Moreover, we request that Ripple take no affirmative action to delete any emails, even emails that may not fit within the parameters set forth above.

While we recognize that this may impose a burden on your client, it is absolutely necessary that Ripple fully comply with their obligations to reasonably retain and preserve Evidence. We appreciate Ripple's efforts in this regard.

If you have any questions or would like to discuss this matter, you may contact me at (212) 336-1012 or waxmand@sec.gov.

Sincerely,

Daphna A. Waxman
Senior Attorney
Division of Enforcement